

RECEIVED
CENTRAL FAX CENTER

NOV 06 2007

IN THE CLAIMS:

Please amend the claims as follows:

1-18. (canceled)

19. (new) A method for encrypting data to be transported between computers, the method comprising:

providing a computer system comprising at least one processor and at least one computer-readable medium operably connected to the at least one processor, the at least one computer-readable memory comprising an input store and an output store;

providing a random number data source running on the at least one processor;

inputting initialization parameters to the random number data source; and

executing, by the computer system, a substitution process comprising

outputting a byte length from the random number data source,

reading, after the outputting, an input string from the input store having a length equal to the byte length,

inputting, after the reading, the input string as an offset to the random number data source,

outputting, after the inputting, a cipher string from the random number data source having a length equal to the length of the input string, and

writing, after the outputting, the cipher string to the output store.

20. (new) The method of claim 19, wherein the computer system further comprises an in-process buffer.

21. (new) The method of claim 20, further comprising
writing, by the computer system, the cipher string to the in-process buffer
providing a test pattern and a determination pattern; and
performing, by the computer system, an obfuscation operation on the cipher string if a first test condition exists, the first test condition being equality of the test pattern to a portion of the determination pattern.

22. (new) The method of claim 21, further comprising:
outputting an obfuscation code from the random number data source; and
wherein performing the obfuscation operation comprises performing a manipulation corresponding to the obfuscation code.

23. (new) The method of claim 22, further comprising:
outputting an obfuscation length from the random number data source; and
wherein performing the obfuscation operation further comprises performing the manipulation on a portion of the cipher string having a length corresponding to the obfuscation length.

24. (new) The method of claim 23, wherein the manipulation is at least one of an exclusive or, a shift, and a substitution.

25. (new) The method of claim 24, further comprising:
repeatedly resetting the test pattern and the determination pattern; and
repeatedly performing the obfuscation operation if the first test condition continues to
exist.
26. (new) The method of claim 25, further comprising inserting an insertion pattern if a
second test condition exists.
27. (new) The method of claim 26, wherein inserting an insertion pattern further
comprises resetting the test pattern and the determination pattern; and
wherein the second test condition is the equality of the test pattern and a portion of the
determination pattern.
28. (new) The method of claim 27, wherein the random number data source comprises a
random pattern generation machine.
29. (new) The method of claim 28, wherein the random number data source comprises a
plurality of random pattern generation machines and an aggregate heterogeneous bit pattern.

30. (new) The method of claim 28, further comprising outputting a pattern from the random pattern generation machine, wherein the random pattern generation machine comprises a pattern table and a logical base and outputting the pattern comprises outputting a pattern from the pattern table corresponding to the logical base and advancing the logical base.

31. (new) The method of claim 30, wherein advancing the logical base comprises modifying a current value according to a rule to obtain a result and storing the result as the logical base.

32. (new) The method of claim 31, wherein:
the plurality of random pattern generation machines comprises a selection random pattern generation machine and a plurality of cipher random pattern generation machines;
outputting the byte length further comprises outputting a selection pattern from the selection random pattern generation machine, the selection pattern corresponding to a first cipher random pattern generation machine of the plurality of cipher random pattern generation machines; and

outputting the cipher string further comprises outputting a pattern from the first cipher random pattern generation machine.

33. (new) The method of claim 32, wherein the selection random pattern generation machine is also a cipher random pattern generation machine.

34. (new) A method for encrypting data, the method comprising:

storing on a computer a data source having a logical base and an offset;

setting the logical base equal to an initial value; and

executing, by the computer, an encryption processes to encrypt clear text, the encryption process comprising

 executing a substitution process comprising

 selecting a segment length,

 reading, after the selecting, a segment comprising a portion of the clear text having the segment length,

 setting, after the reading, the offset equal to a value corresponding to the segment,

 outputting, after the setting, a cipher pattern from the first data source,

 writing, after the outputting, the cipher pattern to an output buffer, and

 advancing, after the outputting, the logical base; and

 repeating the substitution process until the clear text segment has been encrypted in its entirety.